

תל-אביב יפו

עומר עבד אלעזיז אלזהראני, תעודת מעבר קנדית מס' [REDACTED]

המיוצג על ידי בא כוחו עו"ד עלא מחאג'נה ואח'
שייח' ג'ראח, דרך שכס 43, ת.ד. 19870, ירושלים
טל: 02-5824717, פקס: 02-5826010

התובע

-נגד-

1. קבוצת אן. אס. או. טכנולוגיות בע"מ (ח.פ. 514395409)

2. קיו סייבר טכנולוגיות בע"מ (ח.פ. 514971522)

שכתובתן הרשומה היא: גלגל הפלדה 22, הרצליה, 4672222

הנתבעות

מהות התביעה: צו מניעה קבוע/כספית
סכום התביעה: 600,000 ש"ח

כתב תביעה

1. בתביעה זו, התובע יהיה מיוצג ע"י באי כוחו הנ"ל אשר כתובתם להמצאת כתבי בית-דין הינה ככתובת באי כוחם כנ"ל.

2. כל טענה ו/או פרט ו/או עובדה הנטענים בכתב תביעה זה נטענים במצטבר ו/או בהשלמה ו/או לחילופין, הכל לפי העניין ולפי הקשר הדברים ו/או הדבקם.

א. מבוא

3. עניינה של תביעה זו הוא מערכת ריגול מיוחדת-רוגלה-שהנתבעות פיתחו ואשר נעשה בה שימוש כנגד התובע כפי שיפורט בהמשך כתב התביעה. הריגול באמצעות המערכת מתבצע לאחר החדרת תוכנה מרחוק בתוך מכשיר טלפון חכם של האדם שאחריו רוצים לרגל ומבלי לקבל את אישורו. עם סיום התקנת המערכת בתוך המכשיר היא מראה ומשקפת את תוכנו אצל הגוף שמבצע את הריגול.

4. מערכת הריגול-רוגלה- שהנתבעות פיתחו ידועה בשם "פגסוס"- Pegasus (להלן: "המערכת" או "מערכת פגסוס"). המערכת מאפשרת השתלטות על מכשירים ניידים באופן מלא. היא מאפשרת פעולות מעקב פסיביות כגון גישה לשיחות מוקלטות על המכשיר, קבלת גישה לצילומים השמורים במכשיר, גישה להודעות כתובות (טקסט), וגישה לתעבורת אינטרנט. בנוסף, המערכת

מאפשרת גם לשלוט במכשיר באופן אקטיבי, למשל על ידי הפעלת המצלמה מרחוק כדי לצפות בסביבתו של המשתמש.

5. לפי מה שפורסם בכלי התקשורת השונים, הן ברחבי הארץ והן בעולם, מערכת הריגול- הרוגלה שהנתבעות פיתחו נחשבת למתוחכמת ברמה חסרת תקדים והיא עדיפה על רוגלות אחרות מתחרות בשוק. ייחודה של מערכת "פגסוס" נובע מהדרך בה מותקנת בתוך המכשיר, וגם ביכולתה להישאר חבויה מבלי להבחין בקיומה ובפעילותה.

6. לאור אופיה של המערכת, ובהתחשב בפוטנציאל המסוכנות האדיר הטמון בה, ההתייחסות אליה היא כאל נשק, ועל כן מערכת "פגסוס", בדומה לנשק, נמכרת תחת פיקוחו של אגף הייצוא במשרד הביטחון, בהתאם לחוק הפיקוח על ייצוא בטחוני 2007. בהתאם לפרסומים השונים בכלי תקשורת ישראליים, משרד הביטחון מאשר לנתבעות למכור את המערכת רק לגופים ולמדינות מסוימות הנמצאות ביחסים תקינים עם מדינת ישראל.

7. על פיקוח המדינה באשר למכירת המערכת ניתן ללמוד מהעובדה כי ביום 5.7.2018 הותר לפרסום כי הפרקליטות הגישה כתב אישום חמור כנגד אחד מעובדיה לשעבר של הנתבעת מס' 1 שעל פי עובדות כתב האישום העתיק את מערכת "פגסוס" באופן לא חוקי וניסה למכור אותה לגוף זר וללא ידיעת הנתבעות וללא אישור משרד הביטחון. כנגד העובד לשעבר הוגש כתב אישום בעבירות של ניסיון לפגיעה ברכוש שהיה בו כדי לפגוע בביטחון המדינה, גניבה בידי עובד, ביצוע פעולת שיווק ביטחוני ללא רישיון שיווק ביטחוני ושיבוש או הפרעה לחומר מחשב.

=רצ"ב העתק כתבה מאתר "דה מרקר" מיום 5.7.2018 באשר להגשת כתב האישום, מסומן ע/1.

8. הנתבעות מכרו ומוכרות את המערכת לגורמים שונים בעולם, ובהם גופים ממשלתיים ועסקיים. לפי דיווחים שונים בתקשורת, ולפי תלונה שהוגשה ליחידה הארצית לחקירת הונאה במשטרה, הנתבעות מכרו את מערכת "פגסוס" לממלכת ערב הסעודית בשנת 2017 תמורת 55 מיליון דולר ארה"ב.

=רצ"ב העתק תחקיר שהתפרסם בעיתון הארץ ביום 24.11.2018, מסומן ע/2.

9. לפני כשבועיים, ועל רקע גל פרסומים בדבר הפרות זכויות אדם חמורות שהוכח בהן שימוש בתוכנת הריגול שהנתבעות פיתחו, נעשתה פניה אל משרד הביטחון לביטול רישיון הייצוא הביטחוני של הנתבעות. פניה זו שנעשתה בשם הארגון הבינלאומי "אמנסטי" והיא באה על רקע תקיפת סייבר שכוונה נגד אחד מעובדיה כפי שהתפרסם בהודעה שהארגון הוציא ביום 1.8.2018. בהודעה זו נמסר כי היה ניסיון פריצה למכשיר הטלפון השייך לאחד מעובדי הארגון באמצעות מערכת "פגסוס". עוד נאמר בהודעה, כי באותה תקופה פעילים סעודים שנמצאים מחוץ לסעודיה קיבלו הודעות דומות עם קישורים לאתרים שהם חלק מתשתית "פגסוס", דבר המחזק את המסקנה שהמערכת נמכרה לגורמי בטחון בערב הסעודית שמשתמשים בה נגד פעילי זכויות אדם ופעילי אופוזיציה, כדוגמת התובע כפי שיובהר להלן.

=**רצ"ב** העתק הודעות לעיתונות מטעם ארגון "אמנסטי" מימים 26.11.2018 ו- 1.8.2018, מסומן 3/ע.

10. כבר יאמר, בהודעה מפורטת שנמסרה בשם הנתבעות לתקשורת בתגובה לתחקירה הארץ הנ"ל, הן לא התכחשו להתקשרות בינן לבין ערב הסעודית ולעצם מכירת המערכת שהן פיתחו למדינה זו. עצם ההתקשרות לא הוכחש כפי שעולה מהתגובה, וקו ההגנה שהנתבעות דבקו בו היה סביב תרומת המערכת "לאנושות" ולביטחון כדור הארץ! אם כי, הנתבעות הדגישו כי ההתקשרויות נעשות בהתאם לחוק ייצוא ביטחוני ופיקוח משרד הביטחון. יוצא, אפוא, כי הנתבעות מודות למעשה בקיום העסקה עם ערב הסעודית למכירת מערכת "פגסוס".

11. כפי שיובהר להלן, ועל פי דיווחים שונים שהתפרסמו לאחרונה, ערב הסעודית עושה שימוש בתוכנה למעקב אחרי פעילים פוליטיים ומתנגדי המשטר הנמצאים בסעודיה וברחבי העולם כדוגמת התובע שהוא פעיל פוליטי למען דמוקרטיה וזכויות אדם הגולה בקנדה. התובע יטען כי השימוש שנעשה בתוכנה נגדו ונגדו רבים אחרים אינו מתמצא בפגיעה בפרטיותו בלבד, אלא הוא מעמיד אותו ואחרים חפים מפשע בפני סכנת חיים ממשית. **להמחשת הטענה בלבד, התובע יציין כי המערכת שהנתבעות פיתחו שימשה לריגול אחרי השיחות וההודעות הרבות של התובע עם העיתונאי המנוח ג'מאל ח'אשוקג'י שנרצח באופן אכזרי ביותר בתחילת חודש אוקטובר במבנה הקונסוליה הסעודית באיסטנבול. התובע יטען כי הריגול שנוהל אחריו וחשיפת תוכן השיחות וההודעות בינו לבין ח'אשוקג'י באמצעות המערכת תרם תרומה ממשית להחלטה לחסל את מר ח'אשוקג'י על ידי המתנקשים במבנה הקונסוליה.**

12. כפי שיפורט להלן, ובניגוד לנטען על ידי הנתבעות, תפקידן של הנתבעות בפעולות המעקב אינו מסתיים עם מכירת המערכת לגורמים ולמנגנונים שונים, אלא הוא נמשך מעבר לשלב זה והנתבעות ממשיכות לגלות מעורבות אקטיבית בשלבים של העברת הנתונים, עיבוד הנתונים, הדרכה על הפעלת המערכת, וגם סיפוק עדכונים ושדרוג למערכת כפי שמובהר במפרט הטכני הנלווה לחוזה אחר בו התקשרו הנתבעות עם גורמי ממשל במקסיקו במסגרתו מכרו את המערכת תמורה 32 מליון דולרים ארה"ב.

13. התקשרות הנתבעות עם גורמי הממשל במקסיקו עמדה במרכז תביעה אחרת שהוגשה בפני בית המשפט המחוזי בתל-אביב ביום 31.8.2018 (ת"א 61866-08-18). תביעה זו הוגשה בשם של 5 תובעים מקסיקנים כנגד הנתבעות בנוגע למכירת מערכת הריגול "פגסוס" לגורמי ממשל במקסיקו. בדומה למקרה דנן, בתביעה נטען כי נעשה במערכת שימוש למעקב לא חוקי אחרי פעילים פוליטיים וחברתיים דבר שגרם להפרות גסות לזכויות אדם והפרת הזכות לפרטיות של התובעים שהינם פעילים חברתיים ועורכי דין בנושאי זכויות אדם ועיתונאים הלוחמים בשחיתות. בשל חשיבות הסוגיה וחומרתה, פרשת הריגול בזמנו סוקרה בהרחבה בכלי תקשורת ראשיים בעולם. הגשת התביעה בשם התובעים המקסיקנים אף היא סוקרה בהרחבה בכלי תקשורת מובילים בעולם ובארץ.

=**רצ"ב** העתק כתבה שהתפרסמה בעיתון "ניו-יורק טיימס" והעתק כתבות ב"כלכליסט" ו- "דה מרקר", מסומן 4/ע.

התובע

14. התובע הינו תושב קבע בקנדה שמתגורר בעיר מונטריאול בפרובינציית קיבק שבקנדה, והוא גם אזרח של ממלכת ערב הסעודית.
15. בשנת 2009, התובע עבר מסעודיה לקנדה לאחר שהתקבל ללימודים באוניברסיטה במונטריאול. בעת שהייתו במונטריאול כסטודנט, התובע, בעל כשרון רב בשימוש במידיה חברתית, החל להתבטא בנושאים פוליטיים פנימיים בממלכה. הוא החל לספק פרשנות פוליטית באמצעות טוויטר, ואתרי המידיה האחרים. עיקר תרומתו הייתה ביקורת על אופן ניהול המדינה, על משפחה המלוכה השולטת, על השחיתות הגואה בממלכה, ועל מדיניות החוץ של הממלכה. התובע קבל במיוחד על ההפרות הבוטות של זכויות אדם בממלכה ועל הזלזול באזרח הסעודי, זכויותיו וחירויותיו.
16. בשל מעורבותו ופעילותו הפוליטית, ובהתחשב ברמת הפופולאריות שהוא צבר במהרה, הפך התובע למטרה להתנכלויות מצד גורמי ממשל בממלכה. בשל התנכלויות אלה, ובשל הרדיפה הפוליטית שסבל ממנה על ידי גורמי ממשל בממלכה, הגיש התובע בקשת מקלט בקנדה ב- 31.12.2013, בקשה זו התקבלה ביום 21.2.2014. העובדה כי בקשת המקלט שהתובע הגיש התקבלה ובמהרה מלמדת כי רדיפתו הייתה על רקע פוליטי גרידא.
17. בתגובה לרדיפתו הפוליטית, פועלו של התובע כפעיל פוליטי ומבקר חריף של שלטון בית המלוכה הסעודי הלך והתעצם, והוא צבר פופולריות במיוחד בקרב הצעירים בממלכה. לתובע יש כיום יותר מ- 338,000 עוקבים בטוויטר, ולערוץ הווידאו ב- YouTube שהוא מנהל ושבאמצעותו הוא משדר את דעותיו הפוליטיות וביקורתו על המשטר הסעודי יש כ- 141,860 מנויים. בנוסף לשני אמצעים מידיה אלו, התובע תורם ומנהל, ביחד עם פעילים אחרים למען שלטון דמוקרטי בסעודיה, מספר אתרים, חשבונות טוויטר וערוצי YouTube.
18. התובע היה גם חבר קרוב של העיתונאי המנוח ג'מאל ח'אשוקג'י שנרצח באיסטנבול בתחילת אוקטובר השנה באמצעות קבוצת מתנקשים הקשורה למנגנוני הביטחון והביון של ערב הסעודית. משנת 2017, לאחר שמר ח'אשוקג'י עזב את סעודיה ועבר להתגורר בארצות הברית, נרקמה בין השנים מערכת יחסים של ידידות, והם החלו לשתף פעולה במגוון רחב של פעילות פוליטית המיועדת בעיקר לדעת הקהל הסעודית. השותפות הפוליטית הלכה והשתרשה והשניים שיתפו פעולה לפיתוח פרויקטים שונים שטרם יצאו לאור שכן שותפות וידידות זו נקטעה במפתיע לאחר רציחתו של המנוח ח'אשוקג'י באופן אכזרי ביותר בקונסוליה הסעודית באיסטנבול.

הנתבעות

19. הנתבעת מס' 1 הינה חברה הרשומה בישראל. הנתבעת הוקמה בשנת 2010, ע"י היוזמים ניב כרמי, שלו חוליו ועומרי לביא, והחברה נקראת בראשי תיבות של שמותיהם של המייסדים. הנתבעת מפתחת ומשווקת מערכות ריגול למעקב אחרי טלפונים ניידים.

20. הנתבעת מס' 2 הינה חברה הרשומה באותה כתובת של הנתבעת מס' 1, ומניותיה בבעלות מלאה של אותה חברה המחזיקה במניות הנתבעת מס' 1, והדירקטורים הרשומים של שתי החברות הנתבעות הינם אותם אנשים וישויות. על פי פרסומים בתקשורת, הנתבעת מס' 1 ואו בעלי מניותיה ואו מנהליה מנסים להמציא מחדש את המותג של הנתבעת מס' 1 והם עכשיו משווקים אותם מוצרים תחת השם של הנתבעת מס' 2.

=**רצ"ב** פלט מידע על הנתבעות 1 ו- 2 מאת רשם החברות, מסומן ע/5.

21. על פי המידע מרשם החברות, מניות הנתבעת מס' 1 והנתבעת מס' 2 מוחזקות באופן מלא על ידי OSY Technologies S.A.R.L, חברה הרשומה בדוכסות הגדולה של לוקסמבורג ושמספרה הרשום הוא 184226B. חברת האם, OSY Technologies S.A.R.L, הינה בבעלות מלאה של חברת 2 Square, ושמספרה הרשום הוא 192125B ואף היא רשומה בלוקסמבורג. חברת 2 Square היא בבעלות מלאה של חברת Triangle Holdings, הרשומה בלוקסמבורג תחת המספר 192115B, שהיא בבעלות מלאה של Osy Holdings (Cayman), הרשומה באיי קיימן. לפי דו"ח השנתי של OSY Technologies לשנת 2017, שוויה של הנתבעת מס' 2 הינו 408,549,000 דולר ארה"ב (408 מיליון דולר). לפי דיווחים בתקשורת, הבעלים של חברת (Osy Holdings (Cayman הינה חברת Francisco Partners, חברה שמתמחה בהשקעה בחברות פרטיות.

=**רצ"ב** הדו"ח השנתי לשנת 2017 של OSY Technologies, מסומן ע/6.

22. חברת האם, OSY Technologies, גם מחזיקה בחברות אחרות המתמחות בריגול, בין השאר, היא הבעלים של חברת CS Circles Technologies ו- CT Circles Technologies, שתיהן רשומות בלימסול שבקפריסין ומספרן הרשום הוא 336847HE ו- 239933HE בהתאמה. שתי החברות הינן בבעלות OSY Technologies באמצעות החברה הקפאריסאית IOTA Holdings Ltd, אף היא רשומה בלימסול ומספרה 337445HE. הנתבעת מס' 1 היא גם הבעלים של חברת PFOS Technologies Limited, הרשומה בבריטניה ומספרה 8521034. חברות אלו הינן חברות קשורות עם הנתבעות והן פועלות ביחד ומשתפות פעולה במישרים שונים.

23. כך למשל, באחד מהחוזים שהנתבעת מס' 1 חתומה עליו בנוגע להתקשרות בפעילות שלה במדינת איחוד האמירויות הערביות, הנתבעת מס' 1 מתוארת באופן הבא :

"NSO Group Technologies Ltd. ("NSO") and Circles Technologies Ltd. are affiliates of OSY Technologies S.a.r.l ("OSY", and together with any of its affiliates, the "Company")"

=**רצ"ב** העתק מהחוזה מיום 15.8.2016 בין נתבעת מס' 1 לגורם שלטוני באיחוד האמירויות הערביות, מסומן ע/7.

24. התובע יטענו כי לגבי האירועים המתוארים בכתב תביעה זה והמקיס להם עילות תביעה כפי שיפורט בהמשך, נתבעת מס' 1 ונתבעת מס' 2 פעלו כיחידה אחת ובמשותף, וכל פעולה ואו אחריות המיוחסת לאחת מהנתבעות הללו היא גם מיוחסת לנתבעת האחרת.

ג. המסכת העובדתית

מערכת "פגסוס"-PEGASUS

25. הנתבעות הינן המפתחות והמשווקות של המערכת הידועה בשם "פגסוס"- "Pegasus", שהינה טכנולוגית מעקב ברמה צבאית שלפי פרסומי השיווק של הנתבעות, הטכנולוגיה נמכרת בעיקר לסוכנויות ביון וביטחון ממשלתיות ברחבי העולם.

26. המערכות של הנתבעות, בעיקר "פגסוס", נסמכות על מה שידוע בשפה המקצועית כ-" Zero Day vulnerability", שהיא פרצה בתוכנה של המחשב (ובמקרה של הנתבעות, הטלפון החכם) שאינה ידועה ליצרן המכשיר או התוכנה. פרצות אלו מאפשרות לצד הפורץ גישה למידע הנמצא במכשיר ואף שליטה אקטיבית בכל הפונקציות של המכשיר, כגון הפעלת מצלמה, מיקרופון ועוד.

27. לפי המפרט הטכני של "פגסוס", שנחשף כחלק מהתקשרות הנתבעות עם גורמי ממשל במקסיקו, חלק מהמערכת מוחדר לתוך מכשיר הטלפון החכם של היעד באמצעות שתי שיטות, שיטה ראשונה נקראת "Over the Air Programming- OTA", ושיטה שניה מתבצעת באמצעות שליחת מסר SMS לטלפון של היעד או מערכת מסרונים דומה.

28. הנתבעות אף מציעות שירות שהן מכנות (ESEM) "Enhanced Social Engineering Message" שהוא שירות שעוזר למפעיל המערכת לחבר הודעות טקסט במיוחד בהתאם לתחומי העניין של המטרות, על מנת לדרבן אותן מטרות ללחוץ על הקישור המצורף להודעה, דבר המאפשר התקנת המערכת לתוך הטלפון תוך זמן קצר ביותר וללא ידיעת המטרה. במילותיהן של הנתבעות כפי ששירות זה מתואר במפרט הטכני של "מערכת Pegasus מוצע מבחר רחב של כלים כדי לחבר מסרים תמימים שמעוצבים כדי לגרום למטרה לפתוח את הקישור".

=**רצ"ב** העתק המפרט הטכני של מערכת "פגסוס"(בשפה הספרדית והאנגלית), מסומן ע/8.

29. לאחר שהמערכת מוחדרת אל תוך מכשיר היעד, היא מופעלת באופן אוטומטי כדי לנצל פרצות במכשירי הטלפון החכם, והיא מורידה ומתקינה עוד חלקים מהמערכת עד לרמה שבסוף ההתקנה המערכת מצליחה להשתלט על המכשיר מרחוק באופן טוטאלי. כל ההתקנות האלה מתבצעות תוך שניות ומבלי להשאיר סימנים שמערכת הריגול הותקנה בתוך המכשיר.

30. לאחר ההתקנה, ועל פי המפרט הטכני של "פגסוס", המערכת מתחילה מיידית באיסוף נתונים מהמכשיר שהוחדרה לתוכו. לפי המפרט הטכני, הנתונים הללו כוללים את כל המפורט להלן:

- Textual: Textual information includes text messages (SMS), emails, calendar records, called history, instant messaging, contact list, viewing history and much more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
- Audio: Audio information includes intercepted calls, ambient sounds (microphone recording) and other recorded audio files.
- Visual: Visual information includes instant cameras, photo recovery and screenshots.
- Files: each mobile device contains hundreds of files, some invaluable intelligence bears, such as databases, documents, videos and more.
- Location: tracking device location (Cell-ID and GPS) continues.

=**רצ"ב** איור מס' 4 מהמפרט הטכני הנ"ל, מסומן ע/9.

31. הנתונים שהמערכת פגסוס אוספת מתחלקים לשלושה סוגים:

א. **איסוף ראשוני** (Initial Data Extraction) שמתייחס לנתונים שכבר נמצאים על המכשיר ואלה כוללים, רישומי SMS, פרטי קשר, היסטוריית שיחות, רישומי יומן, מסרי דואר אלקטרוני, מסרונים מידיים והיסטוריית דפדוף באינטרנט.

ב. **איסוף נתונים** - ניטור פסיבי (Passive Monitoring) שמתייחס למעקב אחר נתונים חדשים שהמכשיר אוסף תוך כדי שימוש. אלה כוללים את כל הנתונים של האיסוף הראשוני בנוסף למעקב אחר מיקום בהתבסס על ה-cell ID.

ג. **איסוף אקטיבי** (Active Collection), והוא מתייחס ליכולת של המפעיל להנחות את המכשיר הנגוע לאסוף נתונים מהמכשיר וסביבתו הקרובה בזמן אמת. המערכת יכולה לאסוף נתונים הקשורים למיקום, הקלטת שיחות טלפון, העברת קבצים, השימוש במיקרופון כמיקרופון חם לאיסוף והעברת קולות מסביבתו של המכשיר, להשתמש במצלמה לצילום הסביבה, והעברת צילומי מסך של המכשיר הנגוע. הנתבעות מתגאות בכך שיכולת האיסוף האקטיבי היא מה שמבדיל בין "פגסוס" וכל תוכנת איסוף מודיעין מתחרה אחרת.

32. בנוסף לאיסוף נתונים כמפורט לעיל, מערכת "פגסוס" יכולה גם לאסוף נתונים מאפליקציות שנמצאות במכשיר שנפרץ. לפי המפרט הטכני, המערכת יכולה לאסוף מידע מרוב האפליקציות

בעולם. הנתבעות גם יכולות להתאים את המערכת לאפליקציות חדשות על פי בקשת הגוף הרוכש.

=**רצ"ב** פרטי איסוף הנתונים ואופן האיסוף ופעולות ההסוואה מפורטות בטבלה, מסומן ע/10.

33. הנתונים שהמערכת אוספת מועברים מהמכשיר הנגוע לשרתים. אם ההעברה אינה אפשרית הנתונים נשמרים באופן מוצפן על המכשיר שנפרץ עד שיהיה ניתן לשדר נתונים אלה. שמירת הנתונים נעשית באופן מוצפן ובכל מקרה לא תעלה על 5% מהזיכרון הפנוי כדי לא למשוך תשומת לב הבעלים של המכשיר.

34. העברת הנתונים שנאספו מתבצעת בדרך כלל בזמן אמת. האמצעי המועדף הוא Wi-Fi, אך אפשר גם להעביר נתונים באמצעות הרשתות הסלולריות שתומכות 3G, GPRS ו-LTE. אם למכשיר אין גישה לאינטרנט, המערכת יכולה גם לשלוח נתונים באמצעות SMS. כדי להסוות את שידור הנתונים, המערכת מפסיקה כל פעולת שידור כאשר הסוללה מגיעה ל-5% מיכולת הטעינה וגם כאשר המכשיר הנגוע נמצא במצב נדידה. במצב זה, שידור הנתונים מתבצע אך ורק באמצעות Wi-Fi.

35. חשוב לציין כי התקשורת בין המכשיר שנפרץ והשרת המרכזי נעשית באופן עקיף באמצעות רשת אנונימית כדי למנוע אפשרות של מעקב. כחלק מהשירות, הנתבעות בונות רשת שידור שנקראת Pegasus Anonymous Transmission Network שהיא רשת מיוחדת לכל לקוח ולקוח. הרשת מורכבת משרתים שנמצאים במספר מקומות בעולם כך שהנתונים משודרים דרך מספר מסלולים לפני שהם מגיעים לשרתי Pegasus מה שמונע את אפשרות גילוי המערכת.

36. העברת הנתונים מהמכשיר שנפרץ אל השרתים הינה מוצפנת באמצעות AES-128 bit symmetric encryption.

37. היכולת לעלות על כך שמכשיר מסוים נפרץ על ידי מערכת "פגסוס" הינה כמעט בלתי אפשרית שכן המערכת מותקנת בתוך המכשיר ברמת ה-kernel, שהיא תוכנת הליבה המנהלת את ה-CPU (Central Processing Unit) של מכשיר הטלפון החכם. הקרנל שולט בזיכרון ב-CPU וכל פעולות המכשיר. מכיוון שמדובר ברמה הבסיסית ביותר, אי אפשר לגלות את מערכת Pegasus באמצעות מערכת anti-virus או anti-malware.

38. לאחר שהנתונים מועברים לשרתים של מערכת Pegasus, המערכת מציעה מבחר של כלים המאפשרים עיון, מיון, סינון וניתוח הנתונים שנאספו מהמכשיר. המערכת מאפשרת מעקב גיאוגרפי (הן בזמן אמת והן על בסיס מידע היסטורי) כך שכל תנועותיו של המטרה/היעד מוצגות על מפה שהמפעיל יכול לצפות בה. כמו כן, אפשר לעקוב אחר מספר מטרות באותו זמן, ולמייין את המטרות לפי קבוצות. אפשר גם לעשות חיפוש בנתונים כדי לחפש שמות, מספרים או מילות מפתח. כמוכן, המפעילים יכולים לעשות ניתוח של פעולות ותנועות המטרה/היעד על ציר הזמן, ולהנחות את המערכת למסור התראות על התרחשויות אירועים מסוימים כגון קבלת שיחות או הימצאות במקום מסוים. כל הנתונים מוצגים באמצעות ממשק נוח לשימוש וצפיה.

39. כאשר המפעיל מחליט כי אין עוד צורך בריגול אחרי המטרה/היעד, המפעיל יכול להסיר מרחוק את המערכת מהמכשיר שנפרץ. ההסרה נעשית מרחוק ומבלי ידיעת בעל המכשיר או המחזיק בו. במקרים מסוימים המערכת גם יכולה לבצע השמדה עצמית כדי למנוע את גילוייה. בשני המקרים, כאשר חלק זה מהמערכת מוסר מהמכשיר, הנתבעות מציינות במפרט הטכני כי המערכת לא משאירה שום סימן לכך שהמכשיר היה פרוץ באמצעות מערכת Pegasus.

40. כפי שעולה מהמפרט הטכני ומהחווה ההתקשרות עם מקסיקו (הנתבעות הודו בהתקשרויות הללו), מעורבותן של הנתבעות אינה מסתיימת עם מכירת המערכת לגוף המפעיל. הנתבעות מציעות ומספקות גם שירותי תחזוקה, תמיכה, ועדכון/שדרוג לטובת המפעיל. למעשה, הנתבעות מעורבות באופן אקטיבי בפעולות הריגול שהמפעיל מבצע במכשירים שנפרצו.

41. לפי המפרט הטכני, הנתבעות מציעות ומספקות שלוש רמות של תחזוקה ותמיכה. **ברמה הראשונה**, הנתבעות מספקות תמיכה טכנית באמצעות דואר אלקטרוני וגם שיחות טלפוניות. **ברמה השנייה**, הנתבעות מספקות תחזוקה ותמיכה ברמה יותר פרואקטיבית: מהנדסי הנתבעות בוחנים את המערכת ופותרים מרחוק את הבעיות הטכניות שמתגלות באמצעות "תוכנת שולחן עבודה מרחוק ורשת פרטית וירטואלית (remote desktop software and a Virtual Private Network VPN)". **ברמה השלישית**, עבודות התחזוקה שהנתבעות מספקות כוללות תיקון כשלונות של המערכת ושדרוגה.

42. לא זו אף זו, הנתבעות גם מציעות ומספקות תמיכה באתר של המפעיל (בין אם משרד מתוכנן מראש או אתר חירום), וגם השגחה על "בריאות" המערכת ותקינותה.

43. בנוסף לרמת התמיכה הגבוהה שהנתבעות מספקות, הן גם מספקות שדרוג למערכת מספר פעמים בשנה. השדרוגים כוללים פונקציות חדשות שהמערכת יכולה לספק, שדרוגים המאפשרים פריצת מכשירים או תוכנות הפעלה חדשות שהמערכת לא יכלה לפרוץ עד כה, ותכונות המותאמות לצרכים של המפעיל ותיקון באגים המתגלים במהלך הפעלת המערכת.

44. הנתבעות, וכפי שעולה ממסמכי ההתקשרות עם גורמי הממשל המקסיקנים, סיפקו גם, לפי המפרט הטכני, שירותי הדרכה למפעילים המקסיקנים בנוסף לשירותי (configuration) של המערכת.

45. התובע יטען כי כל הפעולות האלה של תמיכה, שדרוג ותחזוקה מעידות על מעורבות מרכזית מתמשכת בפעולות של המפעילים לאחר מכירת המערכת אליהם, כך שכל אי חוקיות שדבקה בפעולותיו של המפעיל אפשר גם לייחס אותה לנתבעות במידה שווה כשותפות שמידת תרומתן הינה מכרעת.

46. כאמור, המידע המפורט הנ"ל באשר למערכת "פגסוס" והמסמכים המצורפים ע/8-10, הינם חלק מהמסמכים שצורפו לתביעה שהגישו התובעים המקסיקנים כנגד הנתבעות בפני בית המשפט המחוזי בתל אביב ביום 30.8.2018.

התקשרות הנתבעות עם גורמי ממשל בערב הסעודית

47. לפני ימים אחדים פורסם תחקיר נרחב בעיתון "הארץ" אודות עסקה במסגרתה הנתבעות התקשרו בחוזה עם הממשל הסעודי למכירת יכולות סייבר התקפיות מתקדמות לסעודיה. מהתחקיר, המסתמך על תלונה ומסמכים שהוגשו למפלג ההונאה במשטרת ישראל ונבחנת בימים אלה, עולה כי הנתבעות התקשרו בעסקה למכירת טכנולוגיה מתקדמת לסעודיים המאפשרת לפרוץ לטלפונים סלולריים, חודשים בלבד לפני שיוש העצר הסעודי החל במסע טיהור כנגד מתנגדיו הפוליטיים.

48. כפי שעולה מהתחקיר, ביוני 2017 נערכה פגישה בווינה בה השתתפו מצד אחד גורמי ממשל סעודים, שכללה לפי הדיווח את בדללה אלמליחי המקורב לראש המודיעין הסעודי שפוטר לאחרונה בעקבות פרשת רציחתו של המנוח ח'אשוקג'י, הנסיך תורכי אלפיסל, ונאסר אלקחטאני שהוא בכיר סעודי המשמש כסגן ראש המודיעין. מצד שני השתתפו אנשי עסקים ישראלים נציגים של הנתבעות. הפגישה הייתה למכירת טכנולוגיה חדישה, מציתת דמיון על פי התיאור, שהנתבעות פיתחו.

49. כעולה מהדיווח, הפגישה עסקה ברכישת המוצר החדש שהנתבעות פיתחו והוא "פגסוס 3", רוגלה מתוחכמת ביותר ביכולתה לפרוץ לטלפון סלולרי מבלי שקורבן הפריצה ילחץ על קישור כלשהו (מספיק לדעת את מספר הנייד בלבד). עוד דווח, כי נציגי הנתבעות ביקשו מהסעודים לרכוש מכשיר טלפון חכם חדש, ולספק להם את מספרו על מנת להוכיח כי "פגסוס 3" מסוגלת לפרוץ אליו רק על ידי מסירת מספר הנייד.

50. לפי התחקיר, הסיפור יצא לאור באמצעות תלונה שהוגשה למפלג ההונאה במשטרת ישראל שהוגשה על רקע סכסוך עסקי בין גורמים שהיו מעורבים בעסקה שנרקמה בין הסעודים לבין הנתבעות. לפי הדיווח, הסעודים הסכימו לשלם לנציג הנתבעות, מר שלו חוליו שהוא גם אחד מהמייסדים של הנתבעות, סך של 55 מיליון דולרים של ארה"ב זאת במהלך פגישה שהתקיימה בערב הסעודית ביולי 2017 במהלכה נרקמה העסקה.

51. תימוכין לידיעות שהובאו בתחקיר הארץ אפשר למצוא בדיווחים אחרים שהיו לאחרונה ובינם פרסומים ב"פורבס" ודיווח של מכון "סטיזון לאב" CITIZEN LAB הקנדי, כפי שיובהר להלן, ולפיהם הנתבעות סייעו למשטר הסעודי לרגל אחרי מתנגדיו. בהתאם לאמור בתחקיר ודיווחים הללו, בין יעדי המעקב היו הסאטירקן ג'אנס אלמסירי ופעיל זכויות האדם יחיא עסירי, שניהם מתגוררים בלונדון, ואת התובע בעצמו החי בקנדה.

52. כאמור, בתגובת הנתבעות לתחקיר הארץ אין הכחשה לקיומה של עסקה בין הנתבעות לבין המשטר הסעודי. כל אשר נטען שם הוא חזרה על אותן סיסמאות ריקות מתוכן, בדבר תרומת הנתבעות והטכנולוגיה שהן פיתחו לאנושות ולהתמודדות עם המציאות הביטחונית בה אנו חיים. הנתבעות שבות ומציינות כי הן פועלות בהתאם לכללי הייצוא הביטחוני ובהנחיית גורמי הביטחון ותחת פיקוחו הצמוד. עוד נמסר בתגובה כי כל אימת בו ישנם דיווחים לניצול המערכת לרעה על ידי מדינה או גוף שרכש אותה, הנתבעות חוקרות את המקרה ונוקטות את הצעדים

הנדרשים והמתבקשים מתוצאות החקירה, לרבות ביטול ההסכמים. כאמור, הנתבעות לא התכחשו לדיווחים כי תוכנות הריגול נמכרו לערב הסעודית כפי שהובא בתחקיר.

53. התובע, שכאמור גולה בקנדה בשל רדיפתו הפוליטית באמצעות גורמי ממשל סעודים, אינו מחזיק בהסכם בו התקשרו הנתבעות עם הממשל הסעודי. יחד עם זאת, ולאור תגובת הנתבעות שנמסרה בתחקיר, ולפיה הן לא התכחשו לחתימת הסכם עם הסעודיים, נדמה כי הנתבעות הן הכתבות הנכונה והראויה ביותר לספק מידע הן באשר לפרטי ההתקשרות עם הממשל הסעודי, והן באשר לתוצאות הבדיקות שנעשו על ידן כביכול בעקבות הדיווחים באשר לשימוש לרעה שנעשה במערכת ששימשה את הסעודיים לצרכי מעקב אחרי מתנגדי המשטר, לרבות התובע עצמו. האם ההסכם עם הסעודים אכן בוטל בעקבות מקרים הללו, ובוודאי בעקבות רציחתו האכזרית של העיתונאי המנוח ח'אשוקג'י? הנתבעות הן אלה שצריכות לספק מידע אודות שאלות הללו ואחרות.

54. כאן המקום לציין כי הנתבעות, גם כאשר עובדת התקשרותן בעסקאות עם ממשלים שעשו שימוש לרעה בתוכנה אינה במחלוקת, כגון המקרה במקסיקו, מסרבות לשתף פעולה עם חקירה פלילית וחקירות רשמיות אחרות שנפתחו במדינות הללו בנוגע לפריצות שדווחו כנגד פעילים פוליטיים וחברתיים. כך לדוגמא, לאחר שהפריצות באמצעות מערכת "פגסוס" נתגלו בעניינם של המקסיקנים, שחלקם הגישו תביעות בפני בית המשפט המחוזי בתל-אביב, נפתחה במקסיקו חקירה פלילית נרחבת סביב הפריצות. באוקטובר 2017, פנו רשויות החקירה במקסיקו באמצעות משרד החוץ בישראל, לקבלת עזרה בחקירה על ידי הפניית שאלון לנתבעת מס' 1 בהתייחס לקשר בינה לבין הרשויות במקסיקו. למרות פניות חוזרות בנובמבר 2017 ובמרץ 2018 מצד שגרירות מקסיקו בישראל, לא נתקבלה שום תשובה לבקשה. הנתבעת מס' 1 לא שיתפה פעולה וכיום, 10 חודשים לאחר הפנייה, היא עדיין מסרבת לשתף פעולה ומסתתרת מאחורי סיסמאות ריקות מכל תוכן. הנתהגות זו מעמידה הצהרות הנתבעות ולפיה "**כל אימת ישנם דיווחים לניצול המערכת לרעה על ידי מדינה או גוף שרכש אותה, הנתבעות חוקרות את המקרה ונוקטות את הצעדים הנדרשים והמתבקשים מתוצאות החקירה, לרבות ביטול ההסכמים**" בסימן שאלה!

55. אשר על כן, לתביעה ולסעדים המבוקשים במסגרתה ניכרת חשיבות מיוחדת בחשיפת האמת והוצאתה לאור, ולא רק לתובע אלא גם להרבה קורבנות אחרים.

פירוט הפגיעות בתובע

56. במרוצת הזמן, ובשל התפתחויות פוליטיות בממלכת ערב הסעודית שלא זכו לתמיכה בקרב הציבור בממלכה, עלה קרנו של התובע והוא הפך לאחד הקולות המשפיעים ביותר בעיצוב דעת הקהל בממלכה בכלל ובקרב הצעירים בפרט. השפעתו של התובע הייתה כה גבוהה עד כדי כך שחברת הייעוץ האמריקאית הגדולה McKinsey & Company תיארה את התובע בדו"ח כאחד משלושת מעצבי דעת הקהל בקשר להתפתחויות בממלכה.

=**רצ"ב** העתק כתבה בניו יורק טיימס מיום 20.10.2018 ומסומן ע/11.

57. בעקבות הדו"ח, אחד משלושת המשפיעים ששם נמסר בדו"ח, מר ח'אלד אל-עלקמי, נעצר. חשבון טוויטר השלישי שהוא בבעלות אנונימית נסגר, ורק התובע היה היחיד מבין שלושת המשפיעים ביותר (על פי הדו"ח) שנותר חופשי להתבטא בענייני המצב בממלכה אך חיו, וכפי שיובהר להלן, הועמדו בסכנה, בין היתר כתוצאה ישירה מפעילות הנתבעות והתקשרותן עם גורמי הממשל בערב הסעודית.

58. באמצע חודש מאי 2018, שני אזרחים סעודים ידועים שיש להם קשרים עם משפחת המלוכה יצרו קשר עם התובע וביקשו להיפגש עמו. בסדרת פגישות שקיימו עמו, שארכו יותר מתשע שעות, השניים הזדהו כשליחיו של יורש העצר הסעודי, הנסיך מוחמד בין סלמאן, ששמו נקשר במתן ההוראה לרציחתו של העיתונאי המנוח ג'מאל ח'אשוקג'י, ושהם עובדים על פי הוראות סעוד אל-קחטאני, שהיה עד לאחרונה היועץ האסטרטגי הבכיר של מוחמד בן סלמאן עד שפוטר מתפקידו לאחר הרצח של מר ג'מאל ח'אשוקג'י וקשירת שמו למעורבות בפרשת הרצח המזעזע.

59. שני השליחים תארו לתובע את מורת רוח יורש העצר הנסיך מוחמד בו סלמאן בכל הנוגע לפעילותו הפוליטית של התובע והביקורת שהוא משמיע כנגד ניהול הממלכה תחת שלטונו של הנסיך, ודרשו ממנו שיפסיק את ביקורתו כלפי המשטר וכלפי יורש העצר. הם דרשו ממנו לחזור לערב הסעודית והציבו בפניו שתי אופציות, הראשונה היא לחזור לממלכה למשפחתו וחבריו, או מאסר.

60. בפגישתם הנ"ל השליחים אף דרשו מהתובע להתלוות אליהם לשגרירות הסעודית בעיר אוטוה לשם השלמת השיחות שם. יצוין כי השניים הביאו עמם אחיו הצעיר של התובע כמסר שהם יכולים לפגוע בבני משפחתו. הזמנת התובע לסור איתם לשגרירות הסעודית לא עוררה דאז חשד בלבו של התובע, יחד עם זאת הוא לא נענה להזמנה וסירב לסור איתם לשם. מאוחר יותר, ועם חשיפת פרשת הרצח המזעזעת של העיתונאי המנוח ג'מאל ח'אשוקג'י, התברר לתובע שייתכן שההחלטה לדחות ההזמנה לסור לשגרירות היא הסיבה שהוא עדיין נמנה בין החיים היום!

61. כאמור, התובע דחה את הבקשה לחזור לערב הסעודית, וסרב להתלוות אליהם לשגרירות ובכך שמר על חיו. הוא המשיך בפעילות הפוליטית שלו, וידידותו ושיתוף הפעולה שלו עם ג'מאל ח'אשוקג'י המנוח הלכו והתהדקו. כך למשל, בחודשים יוני ויולי 2018, עבד התובע עם ח'אשוקג'י על פרויקט "הדבורים האלקטרוניים" שמטרתו הינה לארגן מספר רב של פעילי טוויטר ממתנגדי המשטר בסעודיה כדי להתמודד עם מה שמוכנה "הזבובים האלקטרוניים" שהם קבוצות שפעילי חשבונות טוויטר שלמקבלים הוראות מגורמים במשטר הסעודי ושמטרתם תקיפת פעילי אופוזיציה סעודים והפצת שמועות שליליות נגדם ובאותו עת להלל את החלטותיו ומעשיו של יורש העצר מוחמד בן סלמאן. מר ח'אשוקג'י המנוח אף העביר לתובע סך של 5,000 דולר ארה"ב בתמיכה בפרויקט זה.

62. להערכת התובע, שבדיעבד התברר לו כי פרטי הפרויקט נודעו כמעט בזמן אמת לגורמי הממשל בסעודיה באמצעות המעקב אחריו בשימוש שנעשה במערכת "פגסוס", הפרויקט הנ"ל הרגיו יותר מכל את גורמי הממשל בסעודיה, ולהערכתו גם זהו הפרויקט שעלה למנוח ג'מאל בחייו.

=**רצ"ב** העתק חלק מההתכתבות בין התובע למנוח ח'אשוקג'י, מסומן ע/12.

63. ביום 23.6.2018, קיבל התובע הודעת טקסט שנדמתה להודעה מחברת המשלוחים DHL שבה נאמר: "Dear Customer, DHL shipment No. #1751455027 is scheduled for delivery on 28/6/2018, Manage delivery at <https://sunday-deals.com/tfaEO3gTD>, DHL."

=**רצ"ב** העתק ההודעה מיום 23.6.2018, מסומן ע/13.

64. התובע שבאותה תקופה ציפה להגעת משלוח של מוצרים שקנה באמצעות האינטרנט לחץ על הקישור. לאחר מכן התברר שקישור זה הינו קישור לתשתית מערכת "פגסוס". עם לחיצת קישור זה החדירה המערכת את עצמה למכשיר הטלפון החכם של התובע ובכך נפרץ מכשירו שלא כדין.

65. כתוצאה מפעולות המעקב שבוצעה לאחר שהתוכנה הוחדרה למכשיר הנייד של התובע, בסוף חודש יולי ובתחילת חודש אוגוסט, מסכת ההטרדות נגד התובע על ידי הרשויות בממלכה צברו תאוצה. כוחות הביטחון הסעודיים נכנסו באישון לילה לבית משפחתו של התובע בעיר ג'דה שבממלכה כשהם מלווים בכלבי חיפוש וערכו חיפושים באופן משפיל בכל רחבי הבית. שניים מאחיו של התובע נעצרו ונכון לעת הגשת התביעה הם עדיין במאסר ללא משפט, וכפי שנמסר לתובע, אנשי הביטחון במתקני המאסר מפעילים עליהם עינויים באופן שיטתי בנוסף ליחס בלתי אנושי ומשפיל, הכל במטרה להשפיע על התובע ולהביא להפסקת פעילותו הפוליטית. דפוס התנהגות המתואר של גורמי הממשל כנגד התובע תואם במדויק את הדיווחים של Amnesty International שמתארים כי אנשי הביטחון הסעודיים משתמשים במגוון אמצעי עינויים ותקיפה מינית כדבר שבשגרה בבתי הסוהר ובמיוחד בכלא אל-דיהבאן שבג'דה שם עצורים הרבה פעילים פוליטיים.

=**רצ"ב** העתק דוח Amnesty International מיום 20.11.2018 ומסומן ע/14.

66. בימים הראשונים לאחר מעצר האחים של התובע, אנשי הביטחון הסעודיים הוציאו את אחיו הצעיר של התובע מתא המעצר שלו והורו לו להתקשר לתובע. בהוראת בחוקרים, אחיו של התובע התחנן בפני התובע וביקש ממנו להפסיק את עבודתו על הפרויקטים הפוליטיים בהם הוא מעורב. החוקרים הזכירו במיוחד את פרויקט "הדבורים האלקטרוניים" הנ"ל שהתובע עבד עליו ביחד עם המנוח ח'אשוקג'י ומספר קטן של חברים קרובים. התובע נדהם לגלות שרשויות הביטחון בממלכה יודעים את הכל על פועלו הפוליטי, לרבות פרויקטים בהם הוא משתף פעולה עם אחרים כגון המנוח ח'אשוקג'י, ברמת פרטים קטנים שמספר האנשים שנחשפו אליהם היה מצומצם ביותר. עד אז התובע טרם גילה כי מרגלים אחריו לאחר שמערכת פגסוס שהתנבעות פיתחו הוחדרה שלא כחוק למכשיר הטלפון שלו.

67. גם חלק גדול מחבריו של התובע שמתגוררים בערב הסעודית, שרובם אינם מתעניינים בפוליטיקה בכלל, נעצרו ונחקרו והיו נתונים ליחס בלתי אנושי ומשפיל, הכל במטרה להפעיל לחץ על התובע ולגרום לו לחדול מפעילותו הפוליטית.

68. באמצע חודש אוגוסט קיבל התובע שיחת טלפון ממכון Citizen Lab שהוא חלק מאוניברסיטת טורונטו, ואז נתגלה לראשונה שמכשיר הטלפון שלו נפרץ באמצעות מערכת הריגול שהנתבעות עומדות מאחוריה. למעשה, תוצאות הדוח מהוות עוד הוכחה כי התוכנה אכן נמכרה לשלטונות בערב הסעודית.

=**רצ"ב** העתק דוח מוכן Citizen Lab מיום 1.10.2018 ומסומן ע/15.

69. ביום 2.10.2018, כידוע לכול, נכנס המנוח ג'ימאל ח'אשוקג'י לבניין הקונסוליה הסעודית באיסטנבול ומאז נעלמו עקבותיו. לאחר מספר שבועות התברר שהוא נרצח על ידי צוות חיסול שנשלח במיוחד לרצוח אותו.

70. מר ח'אשוקג'י, שהיה בעברו מזוהה עם נסיכים בבית המלוכה הסעודי ונחשב לבן הממסד, הפך בשנים האחרונות, ובמיוחד לאחר עליית קרנו של יורש העצר, למבקר חריף של השלטון. באמצעות מאמריו והראיונות וההרצאות שהשתתף בהם קרא לרפורמה משמעותית בממלכה שתכלול דמוקרטיה, זכויות אדם, מאבק בשחיתות.

71. הפעילות המשותפת הענפה בין התובע לבין המנוח ח'אשוקג'י הייתה בעלת פוטנציאל אדיר לבניית תנועה פוליטית רחבה למען רפורמות בממלכה שעיקר חבריה יהיו צעירים סעודים נמרצים שכל מטרתם הינה לגרום לשינוי דמוקרטי במדינתם. פעילות המשותפת זו הייתה ידועה על כל פרטיה לרשויות בממלכה באמצעות מערכת "פגסוס" כפי שנחשף.

72. התובע יטען כי השימוש במערכת "פגסוס" והריגול אחר מעשיו וחשיפת שיתוף הפעולה בינו לבין המנוח ח'אשוקג'י תרמו תרומה ממשית לחיסולו. הרי פועלו הפוליטי של המנוח ח'אשוקג'י אינו חדש ורשויות הממשל הסעודים יודעות עליו מזמן, שיתוף הפעולה המתהדק בין התובע לבין המנוח על קידום ופיתוח פרויקטים משותפים היה גורם מכריע להחלטה שהתקבלה להורות על הרצח. התובע יטען כי התקיים קשר סיבתי ישיר בין פעולות המעקב שבוצעה באמצעות מערכת "פגסוס" שבאחריות הנתבעות לבין חיסולו של המנוח ח'אשוקג'י.

73. התובע יטען כי פריצת מכשיר הטלפון החכם שלו על ידי מערכת "פגסוס" הביא לפגיעה בזכויותיו ובפרטיותו, כתוצאה מפגיעה נגרם לו נזק כמפורט בהמשך התביעה.

דפוסי הפעילות והשיווק של הנתבעות וחברות קשורות

74. על אף שהנתבעות והחברות שבבעלותן או חברות הקשורות בהן עוסקות בתחום רגיש במיוחד ועוסקות בפיתוח טכנולוגיה מסוכנת בעלת יכולת לפגוע בזכות לפרטיות של ציבורים בלתי מוגבלים באורח קשה ביותר, הנתבעות והחברות הקשורות שחלקן הוזכר למעלה אימצו דפוסי התנהגות שהפכו לתרבות ארגונית המאופיינת בהפגנת זלזול בזכויותיהם של אחרים ובראשונה הזכות לפרטיות. התנהגות הנתבעות והחברות הקשורות לא משאירה ספקות כי הן מעודדות באופן אקטיבי הפרות בוטות של זכויות אדם, הכל במטרה לשווק את המערכת ובכך להשיג רווח כלכלי גדול יותר.

75. חמור יותר, מסתמן כי הנתבעות, באישור משרד הביטחון, מוכנות להתקשר בעסקאות למכירת מוצריהן למדינות ולמנגנונים מסוכנים ביותר, בתנאי שמדינות הללו נמצאים ביחסים תקינים עם מדינת ישראל, הכל במטרה למקסם את רווחיהן. הסכנה הטמונה בהתקשרויות מסוג זה אינה מתמצא רק בהפרות גסות של זכויות אדם ובראשם הזכות לפרטיות. מתברר, כי המערכת שהנתבעות פיתחו משמשת משטרים, כמו ערב הסעודית, למעקב אחרי מתנגדים פוליטיים וחברתיים דבר שמוביל לפעמים לחיסולם של פעילים אלה כפי שהיה במקרה המזעזע של העיתונאי המנוח ח'אשוקג'י והניסיון שנעשה עם התובע כמתואר לעיל. התובע יטען כי הריגול שבוצע אחריו באמצעות התוכנה שהנתבעות פיתחו היה סיבה ישירה לרציחתו של ח'אשוקג'י, ועל כן המשך השימוש בתוכנה מעמיד אותו ורבים אחרים, פעילים פוליטיים וחברתיים, בסכנת חיים.

76. להמחשת הטענה לקיום דפוס התנהגות המלמד על תרבות המזלזלת בזכות לפרטיות ועל נקיטת אמצעים פסולים במטרה לשווק את המערכת ללקוחות פוטנציאליים מסוכנים נציין הדוגמא הבאה: במהלך שנת 2014 מנהל בחברת Circles Technologies הרשומה בקפריסין, שהיא כאמור בבעלות מלאה של חברת האם של הנתבעות OSY Technologies, ניסה לשדל את הגופים השלטוניים של מדינת איחוד האמירויות הערביות לרכוש מערכת ריגול מהתוצרת של החברה.

77. מהתכתבויות בדואר אלקטרוני בין אריק באנון, מנהל Circles Technologies, לבין אחמד עלי אל-חבסי מהמועצה הלאומית לביטחון לאומי באיחוד, מר אל-חבסי ביקש ממר באנון הוכחה "חייה" על היכולת של המערכת המשווקת באמצעות פריצת וריגול אחרי מספרי טלפון שמר אל-חבסי סיפק למר באנון. בהודעת דואר אלקטרוני מיום 6.8.2014 בשעה 15:08 מאחמד עלי אל-חבסי אל אריק באנון נשלחו 4 מספרי טלפונים לצורך ניסוי המערכת לפני רכישתה.

78. נציגי Circles Technologies עטו על ההזדמנות ובלי היסוס ניסו לספק את הסחורה על ידי פריצת מכשירים אלה! והנתונים שהחברה השיגה כמעוול ראשי נשלחו למר אל-חבסי. התנהגות זו מלמדת בהכרח כי המערכת הוחדרה למכשירי היעד ובכך התאפשר ריגול אחרי בעליהם. מדובר בדוגמא אחת המוכיחה כי הנתבעות אינן ספקיות של המערכת בלבד, כפי שהיחצנים שלהן ניסו לתרץ תפקידן לאחר חשיפת המקרה של התובע בתקשורת ברחבי העולם, אלא מדובר במעוולות ראשיות יחד עם הגוף המפעיל המזמין את המערכת.

=**רצ"ב** העתק התכתבות דואר אלקטרוני מהימים 6.8.2014 ו-10.8.2014 באחמד עלי אל-חבסי לבין אריק באנון ומירוסלב פטריקוב מ-Circles Technologies, מסומן ע/16.

79. סביר להניח גם כי שיטה שיווקית זו אף שימשה הנתבעות להוכחת האפקטיביות של המערכת שעה שמכרו אותה לגורמי הממשל במקסיקו תמורת 32 מליון דולרים, ולסעודים תמורת 55 מליון דולרים! הרי לא יעלה על הדעת כי גורמי ממשל הללו ישלמו הון עתק תמורת המערכת מבלי אף לבדוק את יעילותה ומידת האפקטיביות שלה!

80. כאן המקום לציין גם כי הדוגמא הזו מעלה כי קיים נדבך חשוב נוסף מהשימוש הנועשה במערכת שהנתבעות מספקות. שימוש זה הינו מסוכן כיוון שביכולתו לפגוע בריבונות של מדינות אחרות ונתיניהן.

81. דוגמה נוספת לאדישות הנתבעות כלפי הקורבנות שלה ותרבות הארגונית שלא מתחשבת כלל בזכויות אדם היא המקרה של אחמד מנסור, פעיל זכויות האדם ותושב איחוד האמירויות. על פי דו"ח ארגון Citizen Lab, בשנת 2016, היה נסיון לפרוץ למכשיר הטלפון של מר מנסור, ככל הנראה על ידי שירותי בטחון של האיחוד. מר מנסור נעצר ובחודש מאי 2018 הוא נשפט לעשר שנות מעצר בגלל פוסטים ב-Facebook. מעצרו ומשפטו של מר מנסור סוקרו היטב על ידי ארגוני זכויות אדם בינלאומיים ואף גונו על ידי מומחי זכויות אדם באו"ם.

<https://www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/>

<https://www.hrw.org/news/2018/04/09/uae-one-year-award-winning-human-rights-defender-ahmed-mansoor-whereabouts-remain>

<https://www.bbc.co.uk/news/world-middle-east-39416734>

<https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E>

82. כמו כן, וכפי שצוין לעיל, ארגון זכויות האדם Amnesty International הודיע כי היה ניסיון פריצה למכשיר הטלפון השייך לאחד מעובדיו באמצעות מערכת "פגסוס". הפיתוי שנעשה בו שימוש הפעם היה ידיעה בערבית על הפגנה נגד כליאת פעילים בערב הסעודית. באותה תקופה פעילים סעודים שנמצאים מחוץ לסעודיה קיבלו הודעות דומות עם קישורים לאתרים שהם חלק מתשתית "פגסוס", מה שמוביל למסקנה שהמערכת גם נמכרה לגורמי אכיפה בערב הסעודית שמשתמשים בה נגד פעילי זכויות אדם ופעילי אופוזיציה.

83. מקרים אלה מוכיחים שמערכת "פגסוס" נמכרת לכל מדינה ומשטר הנמצאים בקשרים תקינים עם ישראל - גם אם קשרים אלה אינם גלויים ואין יחסים דיפלומטיים רשמיים - ויש להם את האמצעים לשלם עבור מערכת זו (שעלותה בין 50,000-65,000 דולר לכל פריצה) ללא כל קשר למצב זכויות האדם במדינות אלה וללא נקיטת אמצעי זהירות כלשהם בהעברת המערכת. התקשרות אחת עם משטר כזה הובילה כבר לרציחתו של מתנגד למשטר באופן אכזרי ביותר במקרה שכל העולם שמע עליו והזדעזע ממנו.

ד. עילות התביעה

84. התובע יטען, כי במכירת מערכת "פגסוס" אל גורמי ממשל בערב הסעודית, ובמתן וסיפוק שירותים נלווים אחרים לאחר מכן כפי שפורט לעיל וכמתחייב מההסכם ומהמפרט הטכני הנלווה אליו, הנתבעות פגעו בפרטיותו של התובע והעמידו אותו בפני סכנת חיים, במישרין,

בעקיפין, במעשה או במחדל, ובהתרשלות, ולתובע עומדים עילות תביעה שונות כנגד הנתבעות כדלקמן:

עולה אזרחית בגין פגיעה בפרטיות

85. התובע יטען, כי הנתבעות אשר מכרו מערכת "פגסוס" אל גורמי ממשל בערב הסעודית והמשיכו לספק להם שירותים נלווים בהפעלת המערכת ובהחזקתה, פגעו פגיעה חמורה בפרטיותו ללא הסכמתו ושלא כדין, תוך העמדתו לסכנת חיים.

86. הפגיעה בפרטיותו של התובע הינה ברף החמור ביותר וזאת נוכח מידת החשיפה הרבה שמאפשרת מערכת "פגסוס" במכשיר המיוחדת אליו ושגדו מנוהל המעקב. באמצעות המערכת הזו, הנתבעות יכלו לעקוב אחר הנעשה במכשירים הניידים של התובע בזמן אמת, ואף להפעיל מעקב באופן אקטיבי כפי שהמערכת מאפשרת. מדובר במערכת מסוכנת ביותר וטמון בה פוטנציאל אדיר של יכולת מעקב בלתי מוגבלת אחר חייהם הפרטיים של אנשים נורמטיביים כדוגמת התובע מתוך מטרות ומניעים פוליטיים בראש ובראשונה.

87. אין להכביר במלים באשר למידת הפגיעה בזכותו של התובע לפרטיות נוכח הפעלת המערכת נגדו שכן כל בר דעת יכול לדמיין בראשו את אופיו וטיבו של המעקב שניתן היה לבצע נגדו באמצעות המערכת בזמן אמת.

88. התובע יטען כי הנתבעות פגעו בפרטיותו בשני מישורים עקרוניים, הכל כפי שיפורט להלן:

המישור הראשון, הפרת הפרטיות נעשתה על ידי הנתבעות באופן ישיר ו/או כמעוותות במשותף כלפי התובע עם גורמי ממשל בערב הסעודית. אשר על כן בית המשפט הנכבד מתבקש להטיל על הנתבעות אחריות בגין הפרת החובות המוגנות המפורשות בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות").

המישור השני, הפרת הפרטיות נעשתה על ידי ובאמצעות לקוחות של הנתבעות אשר עושים שימוש בשירותים אותם מספקות הנתבעות, ומשכך חייבות הנתבעות בגין פעילותיהן העקיפות, מכוח אחריותן לפי חוק הגנת הפרטיות ומכוח דוקטרינת ההפרה התורמת. השירותים שהנתבעות מספקות, שכוללים החזקת המערכת ושדרוגה ומתן תמיכה טכנית באופן מתמשך ברמות שונות, כפי שפורט לעיל, אפשרו לגורמי ממשל בערב הסעודית לבצע מעקב אחרי התובע. יצוין, אילולא התרומה המכרעת של הנתבעות לביצוע המעקב, פעולות הריגול כנגד התובע לא היו מבוצעות! מדובר בתרומה מכרעת ואף הכרחית שבלעדיה המעקב לא היה יוצא לפועל. הקשר הסיבתי בין פעילות הנתבעות (ומחדליהן) לבין הנזק הינו חזק וברור. הנתבעות אינן יכולות להסתתר מאחורי הטענה כי במכירת המערכת הן סיימו את חלקן וכי עיקר האחריות רובץ על גורמי הממשל הסעודיים. זוהי טענה שקרית אשר סותרת את האמור במפרט הטכני ונועדה להעביר את האחריות מכתפי הנתבעות.

89. מהתשתית העובדתית כמפורט לעיל עולה כי הוכחו יסודותיה של דוקטרינת ההפרה התורמת: ראשית, התובע יטען כי פרטיותו, כאמור בחוק הגנת הפרטיות, נפגעה על ידי שימוש שעשו גורמי

ממשל בערב הסעודית במערכת שהנתבעות ייצרו ובשירותים אותם הנתבעות מספקות כולל החזקה ושדרוג ומתן תמיכה טכנית. השימוש שעשו גורמי ממשל הללו במערכת שיצרו הנתבעות ובשירותים הנלווים לצורך הפעלתה, הוא זה שהביא לפגיעה בפרטיותם של התובע במובנו של חוק הגנת הפרטיות. למעשה, לא תתכן כלל מחלוקת באשר לפגיעה בפרטיותו של התובע כתוצאה מהשימוש שנעשה במערכת. שנית, הנתבעות הן הספקיות של המערכת והשירותים, תורמים ומעודדים בידעין את הפרת הזכות לפרטיות על ידי המפרים הראשיים - גורמי ממשל סעודים במקרה דנן. לנתבעות ישנה ידיעה ממשית על הסיכון הצפוי בשימוש בשירותים אותן הן מספקות שכן המערכת מיוצרת אך ורק לשם ריגול. פיקוחו של משרד הביטחון על פעולות השיווק של המערכת הוא עוד הוכחה על ידיעת הנתבעות לטיב המוצר שהן פיתחו. זוהי גם הסיבה שהנתבעות דואגות להבהיר כי הן אינן בעלות אחריות לשימוש הנעשה במערכת לאחר מכירתה וכי הן מקפידות על כך שיעשה בתוכנה שימוש לא פוגעני. שלישית, השימוש העיקרי בשירותים אותן הנתבעות מספקות גורם להפרת הפרטיות באופן נרחב בכל רחבי העולם, במיוחד כאשר המערכת נמכרת והשירותים מסופקים למדינות כגון סעודיה ואיחוד האמירויות, שאינן מקפידות, בלשון המעטה, על שמירה על זכויות הנתינים שלהם לפרטיות.

90. התובע יטענו כי לנתבעות קיימת אפשרות שליטה על המידע העובר אל הלקוחות אשר הן מספקות, וכי הן אינן נוקטות אמצעים אקטיביים למניעת ההפרות. תמור יותר, וכפי שצוין לעיל, הנתבעות אינן אף מתעניינות כנגד מי מבוצע המעקב, הן מוכנות לספק השירותים הללו גם במחיר של פגיעה בחפים מפשע.

91. התובע יוסיף ויצוין כי במקרים אחדים, אחד מהם מצמרר במיוחד, כבר הוכח כי פעולות הריגול אחרי מתנגדי המשטר באמצעות "פגסוס" והפרת זכותם לפרטיות הובילה לרציחתם ו/או לכליאתם במקרה הטוב. התובע אמנם דואג לזכותו לפרטיות, יחד עם זאת מדובר בפוטנציאל סכנה גדול יותר שיכול לעלות לו בחייו או בחירותו.

עוולה נזיקית בהתאם לחוק המחשבים, התשנ"ה-1995

92. סעיף 7 לחוק המחשבים קובע כהאי לישנא:

"מעשה מן המעשים המנויים להלן הוא עוולה על פי פקודת הנזיקין [נוסח חדש], והוראותיה של פקודה זו יחולו עליו -

(1) הפרעה שלא כדין לשימוש במחשב או בחומר מחשב, בכל דרך שהיא, לרבות על ידי גזילת דבר המגלם חומר מחשב;

(2) מחיקת חומר מחשב, גרימת שינוי בו או שיבושו בכל דרך אחרת, שלא כדין.

93. התובע יטען כי מעשי ו/או מחדלי הנתבעות כפי שתוארו בפרוטרוט לעיל עולים לכדי עוולה נזיקית במובן סעיף 7 לחוק המחשבים. התובע יטען כי במעשיהם ו/או מחדליהם המתוארים לעיל הנתבעות גרמו להפרעה שלא כדין לשימוש במחשב או בחומר מחשב, לרבות על ידי גזילת

דבר המגלם חומר מחשב. עוד יטענו התובע כי הנתבעות הפרו את הוראת סעיף 7 לחוק המחשבים בכך שגרמו למחיקת חומר מחשב, גרמו לשינוי בו או שיבשו אותו בכל דרך אחרת.

94. התובע יציין כי על הנתבעות רובץ נטל הראיה להראות כי מעשיהם המתוארים לעיל נעשו כדין. החוק מעביר נטל הראיה אל כתפי הנתבעות לבוא ולהוכיח כי מעשיהם ו/או מחדליהם נעשו כדין. העובדה כי שיווק המערכת לגורמים בערב הסעודית קיבל אישור משרד הביטחון אינה מהווה כשלעצמה ראיה לכך כי פעילותיה המתוארים נעשו כדין. דברים הללו נכונים שבעתיים לאחר שהנתבעות ראו בעצמן השימוש שעושה ערב הסעודית במערכת שנמכרה להם! ברור כי המעקב אחריו או אחרי פעילים אחרים אינו נופל בגדר המטרות בהם הנתבעות מתפארות בהגנתן אחרי המוצר שהן פיתחו.

מחדליהם ורשלנותם של הנתבעות

95. מבלי לגרוע מכלליות האמור לעיל, התובע יוסיף ויטען, כי נזקיו נגרמו בשל רשלנותן וחוסר זהירותן של הנתבעות אשר התבטאו, בין היתר, במעשים ובמחדלים כדלקמן:

א. הנתבעות לא פעלו כפי שחברות סבירות, המספקות שירותי סייבר אשר מטיבם וטבעם פוגעים או עלולים לפגוע בפרטיות, אמורות לפעול וצריכות לפעול בנסיבות העניין.

ב. הנתבעות פעלו בחוסר זהירות, תוך הפרה בוטה של הוראות הדין, אשר נועדו לטובת התובע ולהגנתם.

ג. הנתבעות לא נקטו באמצעים מספיקים או הדרושים כדי למנוע את הפגיעה בפרטיותם, כבודם של התובע.

ד. הנתבעות לא קבעו נוהלים והוראות שיבטיחו את השמירה על כבודם, פרטיותם, של התובע.

ה. הנתבעות לא דאגו לבקרה ולפיקוח על הפעילות, הנעשית על ידי הלקוחות שלהן, בשירותים אותם סיפקו.

ו. הנתבעות יצרו מערכת מסוכנת שהשימוש בה עלול לפגוע נאשות בזכותם של התובע ואחרים לפרטיות.

ז. הנתבעות פיתחו ועודדו תרבות של זלזול בפרטיות ואף פגעו בפרטיות לשם הדגמת יכולת המערכת.

ח. הנתבעות המשיכו למכור מערכות ולספק תמיכה ושדרוג מערכות למדינות הידועות בהפרת זכויות אדם גם לאחר שנתגלה שמדינות אלה משתמשות במערכות נגד פעילי זכויות אדם ועיתונאים ובניגוד לחוק.

ט. הנתבעות ולאחר ששמעו וידעו על הזוועות אשר נגרמו על ידי השימוש שנעשה בתוכנה על ידי הממשל הסעודי ועל הריגול הלא חוקי כנגד פעילים פוליטיים, לא ביטלו את ההתקשרות ו/או המשיכו בהתקשרות ובמנן השירותים הנלווים האחרים.

י. הנתבעות סרבו, ועדיין מסרבות, לבקשות רשמיות חוזרות ונשנות לשיתוף פעולה בחקירה פלילית המתנהלת בעניין. הנתבעות מסתפקות בחזרה על סיסמאות ריקות מתוכן באשר לחשיבות התוכנה ותרומתה לאנושות.

יא. מעשיהם אלו של הנתבעות גרמו לתובע נזקים כבדים, והן העמידו את חיי התובע ופעילים רבים אחרים בפני סכנה מוחשית.

יב. התובע יטענו כי החובה לנהוג בזהירות במקרה זה מובהקת, מאחר והנתבעות יצרו את הסיכון שגרם לנזק, קרי, פיתחו ושיווקו את הטכנולוגיה המאפשרת שימוש לרעה.

יג. התובע יטענו כי הנתבעות צפו את ההתנהגות והשימוש לרעה בטכנולוגיה האמורה על ידי לקוחותיה, במיוחד שמדובר בגורמים שיש לגביהם סימני שאלה בדבר מידת שמירתם על זכויות אדם בארצותיהם. עוד יטען התובע, כי הנתבעות וחרף שכבר ידעו כי מדינות מסוימות עושות שימוש לרעה בתוכנה, כפי שנעשה במקסיקו, המשיכו באותה התנהגות והם מכרו מאוחר יותר למדינות אחרות בעולם, כגון ערב הסעודית, שידועות בהפרת זכויות אדם.

96. זאת ועוד, אחריותן של הנתבעות קמה הן באופן ישיר והן כמשדלות ו/או מסייעות (סעיף 12 לפקודת הנזיקין (נוסח חדש), נ"ח התשכ"ח 266 (להלן: "פקודת הנזיקין").

97. התובע יטען כי הנתבעות יצרו מערכת מסוכנת המאפשרת פגיעה קשה בפרטיות ומאפשרת שימוש לרעה המהווה גורם שבלעדיו אין. הטכנולוגיה שהנתבעות מפתחות ומשווקות מהווה גורם שאלמלא קיומו לא היה נזק נגרם והנתבעות היו צריכות לצפות כי טכנולוגיה זו מטיבה ומטבעה תגרום לנזק בגין פגיעה בזכות לפרטיות, במיוחד כאשר היא נמכרת למשטרים עוינים לזכויות אדם, כגון ערב הסעודית. אשר על כן, יטענו התובע כי יש להטיל על הנתבעות אחריות מוחלטת. לחלופין, התובע יטענו להחלת חזקה "הדבר המסוכן" הקבועה בסעיף 38 לפקודת הנזיקין והקובע, כי בהקשר שלנו על הנתבעות נטל הראיה להוכיח שלא הייתה התרשלות וכי נקטו אמצעי זהירות נאותים למניעת הנזק (סעיף 41 לפקודת הנזיקין).

98. התובע יטען כי החובה לנהוג בזהירות במקרה זה הינה מובהקת, מאחר והנתבעות יצרו את הסיכון שגרם לנזק, שכן הן אלה שיצרו את הטכנולוגיה המאפשרת לבצע ריגול אחרי התובע ורבים אחרים בעולם. מתברר, כי עיקר ההתקשרויות עם הנתבעות הינה עם משטרים מפקפקים דבר שאומר דרשני באשר לחובות שההתקשרות הזו מצמיחה כלפי הנפגעים כדוגמת התובע.

99. התובע יטען כי התובעות צפו את ההתנהגות והשימוש לרעה בטכנולוגיה שהן יצרו על ידי צד שלישי אתו הן התקשרו בחוזה. אחריותן של התובעות קמה הן באופן ישיר והן באופן עקיף כמשדלות ו/או מסייעות במובן סעיף 12 לפקודת הנזיקין.

הפרת חובה חקוקה

100. התובע יטען כי באספקת המערכת ובמתן ואספקת השירותים הנלווים לה כפי שתואר לעיל, התובעות אחראיות כלפי התובע בגין הפרת חובה חקוקה לפי סעיף 63 לפקודת הנזיקין. הפרת החובה החקוקה באה לידי ביטוי בהפרת החובות המוטלות על התובעות שלא לפגוע בפרטיותם של התובע וכלל הציבור. לצד הוראות חוק הגנת הפרטיות, התובעות הפרו את חובתן החקוקה שלא לפגוע בזכותם החוקתית לכבוד ולחירות המעוגנת בחוק יסוד: כבוד האדם וחירותו, וכן הפרו את החובה הקבועה בסעיף 2(ג) לחוק האזנת סתר, תשל"ט-1979 שקובעת כי: "המציב או המתקין מכשיר למטרת האזנת סתר שלא כדין או כדי לאפשר שימוש בו למטרה האמורה, דינו – מאסר חמש שנים.", ועוד מספר חקוקים המגנים על החירות ועל חיי אדם ושלומם.

101. התנהגותן של התובעות גרמה לתובעים את הנזק שאותו החיקוק התכוון למנוע. קרי פגיעה בפרטיותם ובכבודם.

מניעת פגיעה עתידית בתובעים ובאחרים

102. התובע יטען כי השירותים אותם התובעות מציעות ומספקות כוללים פוטנציאל לפגיעה עתידית בפרטיות ובזכויות מוגנות אחרות של התובע ושל הציבור בכללותו. פגיעה זו נעשית על ידי התובעות אשר נוכח מעמדן ואופי שירותן, מחויבות שלא לפגוע בזכויות המוגנות של הציבור.

103. אשר על כן, לא די במתן פיצויים לתובע, אשר מטרתו תיקון הנזקים שנגרמו והשבת המצב לקדמותו, התובע מבקשים למנוע פגיעה עתידית בו ובניזוקים פוטנציאליים אחרים, וזאת על ידי מתן צווים אשר ימנעו את המשך אספקת השירותים התובעות מציעות ומספקות למדינות כגון ערב הסעודית. זאת על מנת למנוע את הצורך לחזור ולהגיש תביעות נוספות כגן זו בכל פעם שהשירותים שהתובעות מספקות יפגעו בפרטיותם או בפרטיות אחרים.

החלת עקרונות המשפט הציבורי על התובעות

104. התובע יטען כי לאור העובדה כי הדין אינו נותן מענה מלא למציאות הטכנולוגית המתפתחת היום, יש להחיל עקרונות ונורמות מן המשפט הציבורי על השירותים שהתובעות מציעות ועל פעילותן וזאת נוכח מעמדן ואופי השירותים שהן מציעות ומספקות.

105. התובע יטען כי קיים אינטרס ציבורי כללי ממדרגה ראשונה ביחס לשירותים שהתובעות מספקות, אשר מצדיק החלת סטנדרט ציבורי על תחומי הפעילות של התובעות. כל זאת לאור

האופי המעין ציבורי של הפעילות שהן מספקות ושל תחום ההתמחות שלהן שבדרך כלל הינו נחלת רשויות המדינה וזרועותיה הביטחוניות.

106. לא תתכן כלל מחלוקת כי הנתבעות הינן חברות העוסקות בתחומי ביטחון: הן קרובות וקשורות לזרועות הביטחון במדינה, רבים מעובדיהן הם יוצאי יחידות מודיעין בצבא, והמדינה מתייחסת למוצרים של הנתבעות כאל נשק החייב ברישיון ופיקוח לפי החוק לפיקוח על ייצוא ביטחוני. יצוין, כי ההתקשרות עם גורמי הממשל בערב הסעודית לרוב נעשתה מתוקף הרישיון שקיבלה מאת משרד הביטחון האחראי על מתן רישיונות לחברות ישראליות לייצוא נשק, והעסקה הייתה מפוקחת בהתאם להוראות החוק.

107. את אופיין הציבורי של הנתבעות אפשר ללמוד גם מהמקרה שאירע לאחרונה עת שעובד מפוטר של הנתבעות ניסה למכור את המערכת לצד שלישי, בלי אישור הנתבעות ובלי אישור משרד הביטחון. המדינה התייחסה אל המקרה בחומרה רבה והיא ניהלה מעקב באמצעות השב"כ כנגד העובד עד שנתפס והוגש נגדו כתב אישום חמור במיוחד. סעיפי האישום שהוכללו בכתב האישום מעידים יותר מכל על האופי בטחוני-ציבורי של השירות שהנתבעות מספקות.

108. באופן תאורתי, הנתבעות יכולות להפעיל את המערכת כנגד כל אדם החי בתוך מדינת ישראל או מחוצה לה, ובכך לנהל מעקב מתמשך אחריו ולקבל מידע על פרטים רגילים ביותר הקשורים לחיו האישיים של האדם תחת מעקב. לא יעלה על הדעת לאפשר כוח כזה בידי חברה פרטית מבלי להחיל עליה פיקוח ממשלתי וליישם עליה נורמות וחובות מהמשפט הציבורי. הרי רק מדינות וגופים מורשים על פי חוק ובמקרים חריגים ביותר מוסמכים בצל הגבלות ותנאים לפגוע בפרטיות של אדם. הנתבעות, חברות פרטיות, המחפשות למקסם רווחיהן בכל דרך, אינן אמורות לפעול באופן חופשי מבלי להחיל עליהם אמות מידה החלות על מדינות וגופים ממשלתיים שבידיהן כוח דומה!

109. כבר הוכח כי אי אפשר לסמוך על שיקול הדעת של הנתבעות באשר לבחירת הצדדים איתן הן מתקשרות למכירת מוצריהן! ביותר ממקרה אחד הוכח כבר כי הצדדים אשר קיבלו לידם את התוכנה עשה בה שימוש לרעה והם ניצלו אותה על מנת לעקוב אחרי פעילים פוליטיים, עיתונאים, עורכי דין ומתנגדי משטר.

110. התובע יטען, כי השימוש הנעשה במערכת פגסוס משפיע על כלל הציבור בצורה ניכרת. הכוונה כאן היא לציבור החי במדינת ישראל וגם מחוץ לה בכל אותן המדינות שרכשו את המערכת מאת הנתבעות. בכך הנתבעות נושאות חובה כלפי ציבורים הללו לפעול באופן מידתי, סביר ובתום לב, וכן להימנע מפגיעה בזכויות חוקתיות מוגנות ובעיקר הזכות לפרטיות ובזכות לשם טוב. חובות הללו חלות על הנתבעות באופן מובהק.

111. להמחשת הנקודה, נחזור על סעיפי כתב האישום שהוגש לאחרונה כנגד עובד לשעבר של הנתבעת מס' 1: ניסיון לפגיעה ברכוש שהיה בו כדי לפגוע בביטחון המדינה, גניבה בידי עובד, וביצוע פעולת שיווק ביטחוני ללא רישיון שיווק ביטחוני. סעיפים אלה מעידים כי על אף שמדובר

בחברות פרטיות, בשל רגישות תחום הפעילות שלהן ואפיו הציבורי ומידת המסוכנות הטמונה במוצרים המפותחים על ידי הנתבעות, יש להחיל עליהן נורמות מן המשפט הציבורי.

112. העובדה כי פעילותן של הנתבעות חוסה תחת חוק הפיקוח על ייצוא ביטחוני אף היא מלמדת על אופיין הדואלי של הנתבעות שעל אף היותן חברות פרטיות, מדובר בחברות מיוחדות בעלות מאפיינים של גופים ציבוריים וניתן לראותן כגוף דו מהותי. לחלופין, וגם באם לא מדובר בגוף דו מהותי, התובע יטען כי איסור הפגיעה בפרטיות חל גם על גופים פרטיים ובוודאי חלה על הנתבעות המקבלות רישיון מהמדינה לעסוק בתחומן.

113. התובע יטען, כי בידי הנתבעות פוטנציאל אדיר לפגוע בפרטיותם של אנשים, ואף לגרום לפגיעות חמורות יותר. כפי שהוכח לעיל מההתנהגויות ומדפוסי הפעולה שהנתבעות אימצו, הנתבעות נכשלו לעמוד בנורמות הנדרשות מהן בנוגע לאופן השימוש בשירותים אותם הן מספקות. התובע יטען, כי הנתבעות הפרו ברגל גסה עקרונות אלה הן בכובען כמעוול ראשי והן בכובען כשותפות למעוול ובעלות תרומה מכרעת.

114. התובע יוסיף ויטען, כי המשך הפעלת השירותים של הנתבעות יאפשר לנתבעות ולקוחותיה להמשיך ולפגוע בזכות לפרטיות של התובע ושל רבים אחרים בכל רחבי העולם ובתוך מדינת ישראל, ואף להעמיד חיי אנשים חפשים מפשע בפני סכנה.

הפגיעה בפרטיות והפרת המשפט הבינלאומי

115. התובע יוסיף ויטען כי מעשיהן/מחדליהן של הנתבעות והפגיעה בזכות לפרטיות של התובע מהווה הפרה של סעיף 17 לאמנה הבינלאומית בדבר זכויות אזרחיות ומדיניות משנת 1966 שישאל אישררה ובכך הפכה להיות חלק מהמשפט הפנימי. סעיף 17 לאמנה קובע כי:

1. "לא יהיה אדם נתון להתערבות שרירותית או בלתי-חוקית בצנעת הפרט שלו, במשפחתו, בביתו או בכתובתו, או לפגיעות בלתי חוקיות בכבודו או בשמו הטוב.

2. לכל אדם הזכות להגנת החוק נגד התערבויות או פגיעה כאלה."

116. החובה לכבד הזכות לפרטיות אינה רק נחלתם של גופים ציבוריים או ממשלות. גופים פרטיים, ועל אחת כמה וכמה חברות כגן הנתבעות שיש להן אופי ציבורי מובהק, גם הן חייבות לכבד זכות זו ולתת את הדין על הפרתה. עקרון זה התבסס בשנים האחרונות ובמיוחד לאחר שהאו"ם פירסם את ה- Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and remedy" Framework בשנת 2011.

117. עקרונות אלה מטילים על המדינה ורשויותיה, וכן על הנתבעות, לכבד ולהימנע מלפגוע בזכויות אדם. לגבי עסקים וגופים פרטיים, העיקרון המרכזי כפי שנקבע בסעיף 11 מעקרונות המנחים קובע כי:

"Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."

118. על מנת להבהיר את הנקודה ולהמחשתה, האם מישהו יכול למשל לערער או לפקפק בכך שחברות ענק כגון "פיסבוק", "גוגל" ואחרות מחויבות בכיבוד הזכות לפרטיות של האנשים ברחבי העולם כולו? האם יעלה על הדעת לקבל את הטענה כי החברות הללו אינן ציבוריות ואינן גופים מעין ממשלתיים ועל כן אינן מחויבות בכיבוד זכויות אדם כגון הזכות לפרטיות ובהתאם הן יכולות לעשות ולעוול ולפגוע בזכות לפרטיות ככל העולה על רוחן? בוודאי כי התשובה על שאלה זו הינה שלילית.

119. באשר למדינה, העיקרון המרכזי כפי שבא לידי ביטוי בסעיף 1 של העקרונות המנחים קובע כי:

"States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."

120. התובע יטענו כי חובה זו לשמור ולכבד את הזכות לפרטיות של התובע ואחרים מוטלת גם על בית משפט נכבד זה, וכי חובה זו מחייבת מתן סעד לתובעים כנגד מעלליהן של הנתבעות.

121. יצויין כי טיעון זה אינו נובע מתחום המשפט הבינלאומי גרידא. הזכות לפרטיות מעוגנת במספר מקורות במשפט הישראלי, ויש לה למעמד חוקתי לאחר שנקבע בסעיף 7 לחוק יסוד: כבוד האדם וחירותו כי:

7. (א) כל אדם זכאי לפרטיות ולצנעת חייו.

(ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו.

(ג) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו.

(ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו.

122. משמעותו של עיגון חוקתי זה היא שעיקרון השמירה על הפרטיות צריך להיות עקרון מנחה לבית המשפט כאשר בית המשפט עוסק במלאכת פרשנות החוק ובעת מתן הסעדים הנדרשים.

ה. הסעדים

פיצוי כספי עבור הפגיעה בתובע

123. התובע יבקש מבית המשפט הנכבד לחייב את הנתבעות, ביחד ולחוד, בפיצוי כספי כתוצאה מהנזקים אשר נגרמו לו. כבר יאמר, נזקיו של התובע כתוצאה ממעשיהן ו/או מחדליהן של הנתבעות כמתואר לעיל עולה בהרבה על הסכומים המפורטים להלן. התובע העמיד את תביעתו על הסכומים להלן משיקולים הקשורים בתשלום אגרת בית משפט, ומשיקולים עקרוניים הנובעים מכך שעיקר התביעה הינה קבלת צווי מניעה קבועים כמפורט להלן.

124. התובע יבקש לקבל פיצוי בסך של 550,000 ₪ וזאת בגין הנזקים שנגרמו כתוצאה מהפגיעה בפרטיות ו/או הפרת חוק המחשבים ו/או הפרת חובה חקוקה על ידי הנתבעות ו/או התרשלות שהנתבעות.

125. בנוסף, התובע יבקש לשלם לו פיצוי בסך של 50,000 ש"ח ללא הוכחת נזק בהתאם לסעיף 29א לחוק הגנת הפרטיות.

126. בסך הכל, נכון למועד הגשת תובענה זו, הדרישות הכספיות שהתובע דורש לשלם לו עומדות על סך של 600,000 ₪.

127. בנוסף, בית המשפט הנכבד מתבקש לחייב את הנתבעות בפיצוי לדוגמא עד לגבול סמכותו, מכוח סמכותו הטבועה ולפי שיקול דעתו, זאת בהתחשב בנסיבות המיוחדות של מקרה זה ועל מנת ליצור הרתעה בעתיד מפני המשך דפוס ההתנהגות כפי שתואר לעיל שגורם להפרות קשות ליזכותם של אנשים לפרטיות תוך העמדת חייהם בפני סכנה.

צו מניעה קבוע

128. במקרה דנן, ולאור המקובץ לעיל, התובע יטען כי לא די בתשלום פיצויים. הפיצויים המבוקשים נועדו רק לתקן חלק מהנזקים שנגרמו בעבר בעוד שהצו נועד למנוע את המשך מתן השירותים שהנתבעות מספקות והפוגע בתובע ובזכותו לפרטיות ומעמיד אותו בפני סכנת חיים. על כן, בית המשפט הנכבד מתבקש למנוע את הפגיעה המתמשכת והעתידית העלולה להיגרם כתוצאה מהשירותים שהנתבעות מציעות ומספקות, על מנת למנוע את הצורך לחזור ולהגיש תביעות כגון זו בעתיד, בין אם על ידי התובע ובין אם על ידי אחרים, שמספרם הולך וגדל מיום ליום.

129. התובע מבקש מבית המשפט להוציא צו מניעה קבוע נגד שתי הנתבעות המורה להן:

א. להימנע באופן מוחלט, בין אם במישרין (לרבות באמצעות חברות בת, חברות אם, או חברות אחיות, בארץ ובחו"ל) ו/או באמצעות צדדים שלישיים, ממכירת מערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", לשלטונות בערב הסעודית.

ב. להפסיק לאלתר ובאופן מוחלט, כל פעולת תמיכה, תחזוקה, שדרוג, סיוע, בין במישרין ובין באמצעות צדדים שלישיים, לרבות באמצעות חברות בת, חברות אם, או חברות אחיות, בארץ ובחו"ל, למערכת פגסוס או כל מערכת אחרת שהנתבעות כבר סיפקו לממשל הסעודי, וכל רשות או גוף אכיפה במדינה זו.

130. כן מבקש התובע מבית המשפט להוציא צו קבוע נגד שתי הנתבעות המורה להן:

א. לאסור על לקוחותיהן, או כל משתמש אחר במערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", לפרוץ למכשירי הטלפון של התובע ולהימנע מאיסוף נתונים ממכשירי התובע ו/או העברתם ו/או עיבודם.

ב. לגרום להשבתת ו/או הפסקת הפריצה למכשירי הטלפון של התובע באמצעות מערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", אם פריצה כזו למכשירי הטלפון של התובע עודנה קיימת.

131. להוציא צו מניעה האוסר על הנתבעות למכור את תוכנת פגסוס ו/או כל תוכנת ריגול דומה אחרת למשטרים ו/או מדינות בעולם, אלא לאחר שיובטח כי אותו משטר ו/או מדינה יעשו באותה תוכנה שימוש באופן שאינו סותר את החוק המקומי והבינלאומי, וכן צו המורה לנתבעות לדאוג לכך, שהן בעצמן לא יספקו שירותי תמיכה, תחזוקה, שדרוג, סיוע בתפעול והדרכות לשימוש בתוכנת פגסוס או כל תוכנת ריגול דומה, לאחר שתוכנה כאמור נמכרה לגוף שלישי, אלא לאחר שיוודאו באופן פוזיטיבי ומתמשך כי השימוש שנעשה בתוכנה, נעשה כדין ובהתאם לצווים שיפוטניים של טריבונלים משפטיים מוסמכים באותן מדינות.

132. להוציא צו מניעה קבוע האוסר על הנתבעות למכור את תוכנת פגסוס ו/או כל תוכנת ריגול דומה אחרת למשטרים ו/או מדינות הידועות בהפרות שיטתיות של זכויות אדם.

133. וכן האוסר עליה לתמוך ו/או לתחזק ו/או לשדרג ו/או לסייע בתפעול תוכנת פגסוס או כל תוכנה דומה

סוף דבר :

134. לבית המשפט הנכבד הסמכות העניינית והמקומית לדון בתביעה זו.

135. בהתאם לסעיפים 40 (1) ו- 51(א)(2) לחוק בתי המשפט, נוכח סכום הפיצויים המבוקש, לבית המשפט הנכבד הסמכות העניינית לדון בתביעה.


136. בהתאם לתקנה 3(א)(1) לתקנות סדר הדין האזרחי, תשמ"ד-1984, נוכח מקום מושבם של הנתבעות, לבית המשפט הנכבד הסמכות המקומית לדון בתביעה.

137. אשר על כן, בית המשפט הנכבד, מתבקש לזמן את הנתבעות לדין ולחייבן לשלם לתובע סך של 600,000 ש"ח בצירוף ריבית והפרשים כדין.

138. בנוסף, בית המשפט הנכבד מתבקש ליתן צווי מניעה כאמור בסעיפים 128-133 לעיל.

139. כמוכן, בית המשפט הנכבד מתבקש לחייב את הנתבעות בתשלום הוצאות משפט ושכר טרחת עורכי דין בצירוף מע"מ כדין.

ירושלים 2.12.2018


עלאא מחאג'ינה, עורך דין